IN THE SPECIFICATION:

Please amend the specification as follows:

Please amend page 8, second paragraph, as follows:

A second method of the present invention relates to a method for inquiring of the card issuer about card information if the service provider cannot read a card ~~id~~ ID from a smart card directly, and when application reloading in the smart card is requested by a user.

Please amend the paragraph starting on page 8 continuing to page 9, as follows:

The first method relates to a method by which the card issuer transfers an ~~id~~ ID for uniquely identifying a card, such as a card ~~id~~ ID to the service provider concerned when reissuing the smart card. In this case, the service provider concerned is basically a service provider that has loaded an application in an old card.

If the card issuer notifies these service providers of, for example, information, in which the card ~~id~~ ID of the old card is associated with the card ~~id~~ ID of the reissued card, as reissuance information of the smart card, the service provider can recognize the following facts:

(1) The smart card, which is presented by the card user, is a reissued card.

(2) Information specific to the old smart card that has been previously used by the card user. That is to say, identification data of the smart card, for example, such as a smart card ~~id~~ ID.

Please amend page 9, first full paragraph, as follows:

By knowing the card ~~id~~ ID of the old card, it is possible to check whether or not the application of which loading is requested was loaded in the old card. In addition, if circumstances require, it is also possible to inquire a result of credit investigation of the user, and the like.

Please amend the paragraph starting on page 10 continuing to page 11, as follows:

However, this method is based on the presumption that the service provider can read a card ~~id~~ ID for uniquely identifying the smart card directly from the smart card using an external terminal, or the like. That is because if the card ~~id~~ ID cannot be read, or if the service provider cannot read directly the card ~~id~~ ID that is encrypted using random numbers, collation of smart card reissuance information, which has been notified by the card issuer beforehand, becomes impossible.

Please amend page 11, first full paragraph, as follows:

The second method of the present invention is a method for solving the following problem: the service provider cannot read the card ~~id~~ ID directly from the smart card. In this

case, even if the smart card reissuance information is notified by the card issuer beforehand, the service provider will experience a situation in which, from the smart card, the service provider cannot read data to be inquired. Therefore, a method like the first method described above cannot be adopted.

Please amend the paragraph starting on page 11 continuing to page 12, as follows:

Because of it, an inquiry about the card information is sent from the service provider to the card issuer. When an application reloading request is issued from the card user to the smart card, the service provider obtains information such as a card ~~id~~ ID encrypted from the smart card, and information such as a number described in a card surface, and sends the card issuer an inquiry about ~~id~~ ID information including an "application ~~id~~ ID" for which loading is requested. As a matter of course, the card issuer can recognize a reissued card. The card issuer, therefore, sends a reply that indicates whether or not the smart card is a reissued card. In addition, if the smart card is a reissued card, the card issuer judges whether or not the above-mentioned application was loaded in a corresponding old card. Moreover, if the application was loaded, a "message ~~id~~ ID" used when the old card is permitted to load he "message ~~id~~ ID" is an ~~id~~ ID that uniquely identifies an electronic message used when exchanging the electronic message between the card issuer and the service provider. As an example, there is a method for uniquely identifying the message ~~id~~ ID that uses, for example, company identification data of the card issuer, company identification data of the service provider, and a sequence number of the message in combination. This message ~~id~~ ID enables the service provider to recognize the facts described below. As a numbering method for the message ~~id~~ ID that is unique, there is a method in which company identification data of the card issuer, company information on the service provider, and a sequential number are combined. This method permits an electronic message to be distinguished from the other electronic messages.

Please amend the paragraph starting on page 12 continuing to page 13, as follows:

In this case, the reason why the message ~~id~~ ID is given are the following: because a card ~~id~~ ID cannot be read directly from the smart card, the service provider cannot recognize it even if the old card id is notified; and the card issuer may have a policy that prohibits notification of a card ~~id~~ ID to outside. If the message ~~id~~ ID, which was used when application loading in the old card has been permitted, is used, both of the card issuer and the service provider can recognize it. In addition, the service provider can trace related information including an examination result at that time.

Please amend page 13, first full paragraph, as follows:

Determining which method should be taken as a solution, that is, the first method or the second method depends on characteristics of a smart card used by a system. To be more specific, if companies other than the card issuer are permitted to read a card ~~id~~ ID of a smart card, the first method of the present invention can be used as a solution. On the other hand, if

reading a card ~~id~~ ID is not permitted, the second method of the present invention can be used as a solution.

Please amend page 15, the last full paragraph, as follows:

Fig. 4 is a diagram illustrating a sequence of application reloading, which is used when third parties other than a card issuer can read a card ~~id~~ ID, according to the present invention.

Please amend page 16, the third full paragraph, as follows:

Fig. 8 is a diagram illustrating a sequence of application reloading, which is used when third parties other than a card issuer cannot read a card ~~id~~ ID, according to the present invention.via a reader writer; and the like. The present invention does not relate directly to such operation methods. As a matter of course, the present invention is applicable to all of the cases.

Please amend page 22, the first full paragraph, as follows:

Fig. 2 is a diagram illustrating an outline of an example of a card system. The example shows that there is a chip 21 in a smart card 11, and that the chip 21 exchanges data with a reader writer 22. In the reader writer, there are the following: a control processor 23; a magnetic disk 24 used as a database; and the like. In the smart card 11, as generally shown, terminals such as, for example, Vcc (power supply), GND (ground), RST (reset), I/O (input/output), and CLK (clock) are illustrated. In addition, reference number 25 represents various kinds of inquiries from the reader writer 22 to the smart card 11, for example, inquiries such as a card ~~id~~ ID. A reference number 26 represents a reply that is given by the smart card for the inquiry described above. A general system can be used sufficiently for communication of such various kinds of information.

Please amend page 23, the second full paragraph, as follows:

In addition, in the first method of the present invention, it is possible for a third party other than the card issuer to read the card ~~id~~ ID of the smart card (11) directly. In this case, a typical example of the third party other than the card issuer is, for example, a service provider.

Please amend the paragraph starting on page 24 continuing to page 25, as follows:

More specifically, the "smart card reissuance information" is a list that associates a card ~~id~~ ID of the old card with a card ~~id~~ ID of the reissued card. Fig. 12 shows an example of communication data transmitted and received in a step 403. To be more specific, the communication data is read from, for example, an inventor's database, and is then transmitted. The example of the communication data includes a header, PF ~~(Plattoform)~~ (Platform) type data, information on the old card ~~id~~ ID, information on the reissued card ~~id~~

ID, and the like. By the way, in this case, the PF type data is information for giving an instruction which method should be taken, that is, the first method or the second method, according to the present invention. As a specific example, information such as <100, 200, and 999> is used. For example, <100> indicates the first processing method; <200> indicates the second processing method; and moreover, <999> indicates that a processing method is unknown. Of course, the specific signal example illustrated here is merely one example. Because of it, a system builder can use a desired data configuration. In this manner, the communication data includes pair structured data of the old card ~~id~~ ID and the reissued card ~~id~~ ID. Furthermore, if the card issuer notifies the service provider of the smart card reissuance information, information, which associates the old card with the reissued card, is stored in both of the card issuer database and the service provider database as shown in Fig. 13. The information, which associates the old card ~~id~~ ID with the reissued card ~~id~~ ID, is important for the present invention. After the above-mentioned processing, the processing relating to the reissuance of the smart card ends.

Please amend page 26, starting at the second full paragraph continuing to page 27, as follows:

The service provider requests the reissued card to give a card ~~id~~ ID (step 405). This processing realizes the first method of the present invention. Therefore, the step 405 is an appropriate request because it is based on the assumption that third parties other than the card issuer can read the card ~~id~~ ID directly from the smart card.

The reissued card notifies the service provider of the card ~~id~~ ID of the reissued card (step 406). Generally, such an action is performed by a online system.

The service provider collates a card ~~id~~ ID, which has been read from the smart card, in the smart card reissuance information notified beforehand in the step 403. More specifically, as described above, the "smart card reissuance information" is a list that associates a card ~~id~~ ID of the old card with a card ~~id~~ ID of the reissued card. Figure 12 shows this example. If the card is a reissued card, an ~~id~~ ID of the reissued card exists in the smart card reissuance information. According to the data in which both ~~ids~~ IDs correspond to each other, a card ~~id~~ ID of the corresponding old card can be checked. The service provider reads information on the old card from a database, or the like, of the service provider using the card ~~id~~ ID of this old card as a key. According to this search result, the service provider checks whether or not the application, of which reloading is requested by the user, was loaded in the old card. In addition, the examination result obtained when loading the application in the old card is utilized. Information required for application reloading, such as account information in a case where loading is charged, is inquired and used for reloading. Thus, if the application is judged to be reloadable, the service provider reloads the application in the reissued card (step 407).

Please amend the paragraph starting at page 27 continuing to page 28, as follows:

In addition, as an embodiment of this method, an irregular example as shown in Fig. 19 can also be considered. A difference from Fig. 4 is that a step 408 and a step 409 are added instead of the step 403. In other words, in the method shown in Fig. 4, the service

provider notified the card issuer concerned of smart card reissuance information beforehand. And the service provider collated the old card ~~id~~ ID with the reissued card ~~id~~ ID in own system.

Please amend page 28, first full paragraph, as follows;

On the other hand, in the method of Fig. 19, when the user requests the service provider to reload the application, the service provider transmits the reissued card ~~id~~ ID to the card issuer, and requests the card reissuance information. Because of it, timing in transmitting the smart card reissuance information is different.

Please amend page 28, the second full paragraph, as follows:

However, in both of the embodiments, data having a structure, which includes the old card ~~id~~ ID and the reissued card ~~id~~ ID as a pair, is given from the card issuer to the service provider as smart card reissuance information. Both of the embodiments are the same on this point.

Please amend the paragraph starting on page 15 continuing to page 29, as follows:

Fig. 14 shows an example of data related to the smart card, which is stored in the database by both of the card issuer and the service provider. The example of the data is stored using a card ~~id~~ ID as a key, and includes user information, and information relating to a loaded application (for example, a loaded application ~~id~~ ID, etc.). Moreover, the data includes information of examination that is performed according to a company's policy when loading the application. If loading of the application is charged, its accounting information, and the like, is also included. It is to be noted that, as a matter of course, a real system may includes additional information, and various kinds of information, of which configuration is different from that of information illustrate in this example.

Please amend page 30, first full paragraph, as follows:

Fig. 7 is a flowchart illustrating operation of the "service provider" in a case where application reloading processing is performed for the reissued card in response to a request from the user. The service provider receives an application reloading request from the user (step 701). The service provider requests the smart card to notify a card ~~id~~ ID (step 702). The card ~~id~~ ID is received from the smart card (step 703).

Please amend page 30, second full paragraph, as follows:

As show in the step 601 in Fig. 6, the card ~~id~~ ID is received from the card issuer. The card id of the reissued card is searched in the smart card reissuance information, which is stored in the smart card application management database (step 704).

Please amend page 30, third full paragraph, as follows:

If the card ~~id~~ ID does not exist in the database, it is possible to conclude that the card is not a reissued card, or that the service provider has not loaded the application in the old card. Therefore, the application reloading processing is cancelled, and the user is notified of it (step 707). If the card ~~id~~ ID exists in the smart card application management database, the service provider searches card information on the old card in the smart card application management database using a card ~~id~~ ID of the corresponding old card as a key (step 706).

Please amend page 31, first full paragraph, as follows:

Next, a sequence of the second method according to the present invention will be described with reference to Fig. 8. The second method is a method for realizing application reloading processing for a smart card type, which does not permit third parties other than a card issuer to read a card ~~id~~ ID directly. A reason why the third parties are not permitted to read the card ~~id~~ ID directly is thought that the card issuer has a policy to prevent people outside from knowing the card ~~id~~ ID for security reasons.

Please amend page 32, first full paragraph, as follows:

Application is reloaded on the assumption that this application was loaded in the old card. When loading the application in the old card, the card issuer and the service provider exchange permission for loading, and share identification data of an electronic message for the permission (that is, an ~~id~~ ID).

Please amend page 32, third full paragraph, as follows:

In contrast to the first method of the present invention, the card issuer does not notify the service provider of smart card reissuance information in this method. That is because even if a list relating to the card ~~id~~ ID of the smart card is notified, the service provider cannot read the card ~~id~~ ID from the smart card. Therefore, collation becomes impossible. All of the processing relating to card reissuance ~~were~~ is described above.

Please amend the paragraph starting at page 33 continuing to page 34, as follows:

The service provider requests the reissued card to give card attribute data (step 804). The processing realizes the second method of the present invention. The card outputs the attribute data such as the card ~~id~~ ID to outside in the form that can be identified only by the card issuer. In this case, the "card attribute data" is information that identifies the smart card. In other words, the card attribute data is data that is loaded in the smart card, and that permits this smart card to be distinguished from other smart cards. As an example, there may be a method in which the card ~~id~~ ID is encrypted using a public key of the card issuer. As another example, there is a card ~~id~~ ID that is encrypted by the card issuer using the card issuer's own public key. The encrypted card ~~id~~ ID is loaded in the smart card by the card issuer in card issuance processing. As a matter of course, it is needless to say that other encrypting

methods can also be used. The reissued card notifies the service provider of the card, attribute data that can be decrypted only by the card issuer as described above (step 805). Generally, such data is notified by an online system.

Please amend the paragraph starting at page 34 continuing to page 35, as follows:

The service provider transmits the card attribute data, and the application ~~id~~ ID for which reloading request is issued, to the card issuer, and requests for inquiry about card information (step 806). Although the service provider cannot decrypt the card attribute data, the card attribute data can be decrypted by the card issuer. Therefore, the card issuer reads information on the old card corresponding to the reissued card from the smart card management database using the card attribute data, which has been sent, as a key. The message ~~id~~ ID which is used when permission for loading has been exchanged between the card issuer and the service provider, is also searched; the permission for loading is required to load the transmitted application in the old card in like manner (the "message ~~id~~ ID is an electronic message ~~id~~ ID exchanged between the card issuer and the service provider, and permits an electronic message to be distinguished from other electronic messages uniquely). The card issuer transmits the following to the service provider (step 807): information on whether or not a card for which inquiry is requested is a reissued card; and if it is the reissued card, a message ~~id~~ ID used when the permission for loading the application, for which reloading is requested, in the old card has been exchanged.

Please amend page 35, first full paragraph, as follows:

Fig. 15 shows an example of communication data transmitted and received in a step 807. The communication data includes, for example, a header, a PF type, capability to reissue OK/NG, and a message ~~id~~ ID and the like. In this case, the header and the PF type are the same as those described above. In this manner, the communication data includes "capability to reissue OK/NG" information; to be more specific, the message ~~id~~ ID and information on whether or not it is a reissued card. According to the received information, the service provider checks the following: whether or not the smart card is a reissued card; and whether or not the application, for which reloading is requested, was loaded in the old card.

Please amend the paragraph starting at page 35 continuing to page 36, as follows:

In addition, as a result of notifying the smart card reissuance information, as shown in Fig. 16, in both of the card issuer database and the service provider database, the capability to reissue OK/NG is stored; more specifically, the information on whether or not it is a reissued card is stored, and in addition to it, if it is the reissued card, the message ~~id~~ ID associated with the reissued card is stored. Moreover, they can read the data mutually. In addition, the service provider can obtain information at the time of loading in the old card, such as an examination result, by searching the smart card application management database using the message ~~id~~ ID, which is used when the permission for loading in the old card has been exchanged, as a key. The processing described above enables the service provider to check

whether or not the application, of which reloading is requested by the user, was loaded in the old card. In addition, the service provider can inquire information required for application reloading, such as an examination result at the time of loading, to judge whether or not the application is reloadable. If it is judged to be reloadable, the card issuer reloads the application in the reissued card (step 808).

Please amend page 36, first full paragraph, as follows:

Fig. 17 shows an example of data related to the smart card, which is stored in the database by both of the card issuer and the service provider. The example of the data is stored using a message ~~id~~ ID as a key, and includes user information, and information relating to a loaded application, such as a loaded application ~~id~~ ID. Moreover, the data includes information of examination that is performed according to a company's policy when loading the application. If loading of the application is charged, its accounting information, and the like, is also included. As a matter of course, other information may also be held arbitrarily as desired.

Please amend page 37, first full paragraph, as follows:

Fig. 9 is a flowchart illustrating operation in the "card issuer", which performs the processing of the second method according to the present invention. The "card issuer" receives a card reissuance request from the card user (step 901). The card issuer examines the card reissuance request according to the card issuer's own operation policy (step 902). If reissuance is not permitted as a result of examination, the card issuer cancels the card reissuance processing, and notifies the user of it (step 904). If the reissuance is permitted as a result of the examination, the card issuer reissues a smart card to the user (step 903). After that, the card issuer stores the smart card reissuance information in the smart card management database, etc., and ends the smart card reissuance processing (step 905). More specifically, the smart card reissuance information is a list that associates a card ~~id~~ ID of the old card with a card ~~id~~ ID of the reissued card.

Please amend the paragraph starting at page 37 continuing to page 39, as follows:

Fig. 10 is a flowchart relating to the "card issuer", in which processing for a card information inquiry request issued by the service provider for a reissued card is shown. The card issuer receives the card information inquiry request for the reissued card from the service provider (step 1001). The card information inquiry request includes card attribute data, which' has been read from the smart card by the service provider, and an application ~~id~~ ID of which reloading is requested. Because the card attribute data is usually encrypted, or is processed by another method, only the card issuer can decrypt the data. Therefore, the card attribute data is decrypted, and using the decrypted data as a key, the smart card management database is searched (step 1002). The service provider is notified that the smart card is not a reissued card, in the following case: if information corresponding to the card attribute data does not exist in the smart card management database; or if a corresponding smart card is an initially issued card that is normal; or if it is a reissued card, but if the application which

corresponds to the application ~~id~~ ID received in the step 1001 is not loaded in a corresponding old card. After the notification, the processing ends (step 1005). If the information corresponding to the card attribute data exists in the smart card management database, the message ~~id~~ ID, which is used when the application having the application ~~id~~ ID received in the step 1001 has been loaded in the corresponding old card, is searched. Then, information indicating that the card is a reissued card, and the message ~~id~~ ID used when the application of which reloading is requested has been loaded in the old card, are transmitted to the service provider before the processing ends (step 1004).

Please amend page 39, first full paragraph, as follows:

Fig. 11 is a flowchart illustrating operation of the "service provider" when reloading an application in a reissued card in like manner. The service provider receives an application reloading request from the user (step 1101). The service provider requests the smart card to transmit card attribute data (step 1102). The card attribute data is received from a smart card (step 1103). A card information inquiry request relating to the reissued card is sent to the card issuer (step 1104). The request includes the card attribute data, and an ~~id~~ ID of an application for which the reloading request is issued.

Please amend the paragraph starting at page 39 continuing to page 40, as follows:

A result of the card information inquiry is received from the card issuer (step 1105). As a result of the inquiry, if the smart card is not a reissued card, the processing of reloading the application in the smart card is cancelled, and then the user is notified of it (step 1107). As a result of the inquiry, if the smart card is a reissued card, loading permission has already been exchanged when reloading the application, for which the reloading request was issued, in a corresponding old card. Because the exchanged message has already been received from the card issuer, the smart card application management database is searched using the message ~~id~~ ID as a key (step 1106). Then, the examination result obtained when the application has been loaded in the old card is referred to. In addition, if there is a charge, accounting information is also referred to. If the application, for which a reloading request is issued, was loaded in the old card successfully, examination information on loading of the application in the old card is judged. In addition, if there is a charge, accounting information, and the like, is referred to. If the application is judged to be reloadable, the application is reloaded in the smart card, and the processing ends (step 1108).

Please amend the paragraph starting at page 40 continuing to page 41, as follows:

Selection of which method should be used (that is, the first method or the second method of the present invention) depends on a card handled by the system. To be more specific, if a card ~~id~~ ID of the smart card can be read by third parties other than the card issuer, the first method may be used. If it is possible to read the card attribute data that can be decrypted only by the card issuer, the second method may be used. In addition, if the system handles two or more kinds of smart cards, and if the system handles both of a smart card type using the first method and a smart card type using the second method, this problem can be

solved by including platform type data, which indicates the kinds of the smart cards, in communication data exchanged between the card issuer and the service provider. Figs. 12 and 15 illustrate examples of the communication data that include the platform type data. The company, which receives the communication data, judges which processing should be performed (that is, the processing by the first method or the processing by the second method) by referring to the platform type data.

Please amend page 41, first full paragraph, as follows:

As described above, the communication data, which contains the platform type data, is exchanged between players, that is to say, between the card issuer and the service provider. The card issuer or the service provider, which receives this communication data, is described using an operation flowchart (Fig. 18). In the first place, the communication data is received, and then the platform type data contained in the data is referred to (step 1801). Whether or not a card ~~id~~ ID of the smart card currently being processed can be read by companies other than the card issuer is judged using the platform type data (step 1802). If the card ~~id~~ ID can be read, the first processing of the present invention is performed (step. 1803). If the card ~~id~~ ID cannot be read, the processing in the second embodiment according to the present invention is performed (step 1804). When exchange the communication data between the card issuer and the service provider, two or more kinds of smart cards can be handled by performing the processing shown in Fig. 18 before everything else.

Please amend page 42, first full paragraph, as follows:

According to present invention, if the user wants to load an application in a reissued card dynamically, the service provider, which accepts the loading request, can know by the present invention that the smart card is the reissued card. In addition, it becomes possible to verify whether or not the application reloading request from the user is an appropriate request. Moreover, according to the present invention, the above-mentioned verification is possible in both cases: in a case where third parties other than the card issuer can read the card ~~id~~ ID and in a case where the third parties cannot read the card ~~id~~ ID.

Please amend page 44, first full paragraph, as follows:

In other words, this form is a database in a smart card issuance/management system characterized in that

said database includes a message ~~id~~ ID for uniquely identifying an electronic message exchanged with a service provider;

said message ~~id~~ ID has been provided when loading an application in an old card corresponding to a reissued card, as information related to the reissued card, for the purpose of associating the reissued card with the old card when reissuing a smart card; and

a search using a reissued card ~~id~~ ID as a key permits the message id to be extracted. In this case, extraction of the message ~~id~~ ID means that included data is searched by

contrasting the card ~~id~~ ID with the message ~~id~~ ID using, for example, the reissued card ~~id~~ ID held in a hard disk, etc. as a key.

Please amend the paragraph starting at page 44 continuing to page 45, as follows:

In other words, this form is a database in a smart card service providing/managing system characterized in that

said database includes a message ~~id~~ ID for uniquely identifying an electronic message exchanged with a card issuer;

said electronic message has been provided when loading a requested application in an old card corresponding to a reissued card, as data received from the card issuer as smart card reissuance information, when an application loading request is issued by a user to a reissued card; and

a search using this message ~~id~~ ID as a key permits information, which relates to application loading when loading the application in the old card, to be extracted.